IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

DANIEL B. STORM, HOLLY P. WHITE, DORIS MCMICHAEL, and KYLE WILKINSON, individually and on behalf of all others similarly situated, Plaintiffs,	:	14-cv-1138
v.	:	
PAYTIME, INC., Defendant.	:	
	:	Hon. John E. Jones III
BARBARA HOLT and LINDA REDDING, individually and on behalf of all others similarly situated, Plaintiffs,	:	
v.	:	
PAYTIME HARRISBURG, INC., d/b/a PAYTIME, INC., a Pennsylvania corporation, Defendant.	:	

MEMORANDUM

March 13, 2015

There are only two types of companies left in the United States, according to data security experts: "those that have been hacked and those that don't know

they've been hacked."[1] According to a 2014 report conducted by the Ponemon Institute, 43% of companies have experienced a data breach in the past year. Even worse, the absolute size of the breaches is increasing exponentially.[2] When our fellow citizens hear statistics such as these, they are understandably worried about the privacy of their most personal information, such as their Social Security numbers and bank account information. Further, when a data breach occurs, especially one intentionally done by a hacker, it is not unreasonable for the victims to feel that a wrong has clearly been committed. But has there been an actionable harm that is cognizable in federal court? This is the question with which we must grapple in the matter *sub judice*.

Pending before the Court are two putative class actions concerning a security breach of Defendant Paytime, Inc.'s ("Paytime") computer systems, in which an unknown third party allegedly accessed Plaintiffs' confidential personal and financial information. These cases have been consolidated. Prior to consolidation, Paytime filed in each case a Motion to Dismiss Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), contending that Plaintiffs lack standing, or in the

---

[1] Nicole Perlroth, *The Year in Hacking, by the Numbers*, N.Y. TIMES, Apr. 22, 2013, http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_r=0.

[2] Elizabeth Weise, *43% of Companies Had a Data Breach in the Past Year*, USA TODAY, Sept. 24, 2014, http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/.

alternative, that they have failed to state claims as a matter of law. Paytime also filed a Motion to Strike Class Allegations Pursuant to Federal Rule of Civil Procedure 12(f) in each case. For the reasons that follow, we will dismiss the consolidated case for lack of standing, and accordingly, not address Paytime's other motions.

I. PROCEDURAL HISTORY

On February 18, 2015, *Storm, et al. v. Paytime, Inc.* and *Holt, et al. v. Paytime, Inc.* were consolidated into one case for the remainder of the proceedings between the parties. (*Storm*, Doc. 46). However, due to the fact that these cases were filed separately and have had filings and motions pending in separate dockets, we will discuss their procedural histories separately.

In *Storm*, on June 13, 2014, Plaintiffs filed a Complaint against Paytime, alleging claims of negligence and breach of contract. (*Id.*, Doc. 1). The Complaint also included class action allegations under Federal Rule of Civil Procedure 23. Plaintiffs allege that as many as 233,000 individuals could be members of the class, as that is approximately how many individuals who had their personal and financial information allegedly compromised.

By agreement of the parties, Paytime's response to the Complaint was due August 1, 2014. (*Id.*, Doc. 7). On that date, Paytime filed a motion to dismiss for

failure to state a claim upon which relief may be granted and for lack of standing. (*Id.*, Doc. 12). In response to this motion, Plaintiffs filed an Amended Complaint on August 8, 2014. (*Id.*, Doc. 17). Again by agreement of the parties, Paytime's response to the Amended Complaint was due August 27, 2014. (*Id.*, Doc. 18).

On August 27, 2014, Paytime filed the instant Motion to Dismiss for failure to state a claim and for lack of jurisdiction. (*Id.*, Doc. 28). On the same date, Paytime filed its brief in support of the Motion. (*Id.*, Doc. 29). After being granted an extension of time to file its response, Plaintiffs filed their brief in opposition to the Motion on September 24, 2014. (*Id.*, Doc. 37). Paytime filed a reply brief on October 7, 2014. (*Id.*, Doc. 41). Thus, having been fully briefed, this Motion is now ripe for our review.[3]

Turning to the procedural history of *Holt et al. v. Paytime*, Plaintiffs in that case originally filed their putative class action lawsuit against Paytime in the United States District Court for the Eastern District of Pennsylvania on June 27,

[3] In addition to the Motions to Dismiss, Paytime also filed Motions for Leave to File a Third Party Complaint. (*Storm*, Doc. 38; *Holt*, Doc. 31). Paytime seeks to join Netcomm Solutions, Inc., d/b/a SotirIS Information Strategies ("SotirIS") as a Third Party Defendant. Paytime filed briefs in support of these Motions. (*Storm*, Doc. 39, *Holt*, Doc. 32). However, Plaintiffs never filed briefs in opposition to these Motions, and their time do so has long expired. Pursuant to Local Rule 7.6, the Motions are deemed unopposed. While we ordinarily would grant an unopposed motion, because we will be granting the Motions to Dismiss in their entirety, the Motions for Leave to File a Third Party Complaint are now moot and should be dismissed as such.

2014. (*Holt*, Doc. 1). In their Complaint, they alleged causes of action under breach of contract and Pennsylvania's Unfair Trade Practices and Consumer Protection Law (UTPCPL). On August 4, 2014, Paytime filed a Motion to Dismiss Pursuant to Federal Rules of Civil Procedure 12(b)(1) & 12(b)(6). (*Id.*, Doc. 5). A day later, on August 5, 2014, Paytime filed a Motion to Transfer Venue to the Middle District of Pennsylvania. (*Id.*, Doc. 6). On September 3, 2014, Plaintiffs filed their brief in opposition to the Motion to Dismiss. (*Id.*, Doc. 12). Paytime filed its reply brief on September 11, 2014. (*Id.*, Doc. 18).

By court order, on September 26, 2014, *Holt* was transferred to the Middle District of Pennsylvania. (*Id.*, Doc. 21). The matter was filed in this Court on October 10, 2014. (*Id.*, Doc. 22).

Because the Motion to Dismiss pending in *Holt* has been fully briefed, this matter is also ripe for our review, as part of the consolidated case.

II. STANDARD OF REVIEW

Because we need only address Paytime's jurisdictional arguments, Federal Rule of Civil Procedure 12(b)(1) provides the relevant legal standard.

A court must grant a motion to dismiss if it determines it lacks subject matter jurisdiction to hear a case. *See* FED. R. CIV. P. 12(h)(3). A motion to dismiss based on a lack of standing is a jurisdictional matter and thus "properly brought pursuant

to Rule 12(b)(1)." *Ballentine v. United States*, 486 F.3d 806, 810 (3d Cir. 2007). When considering a motion to dismiss under Rule 12(b)(1), a court must distinguish between facial and factual challenges to its subject matter jurisdiction. *See Mortensen v. First Fed. Sav. & Loan Ass'n*, 549 F.2d 884, 891 (3d Cir. 1977). A facial attack challenges whether the plaintiff has properly pled jurisdiction. *Id.* "In reviewing a facial attack, the court must only consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." *Gould Elecs., Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000) (citing *Mortensen*, 549 F.2d at 891). A factual attack, in contrast, challenges jurisdiction based on facts apart from the pleadings. *Mortensen*, 549 F.2d at 891. "When a defendant attacks subject matter jurisdiction 'in fact,' . . . the Court is free to weigh the evidence and satisfy itself whether it has power to hear the case. In such a situation, 'no presumptive truthfulness attaches to plaintiff's allegations, and the existence of disputed material facts will not preclude the trial court from evaluating for itself the merits of jurisdictional claims.'" *Carpet Group Int'l v. Oriental Rug Importers Ass'n*, 227 F.3d 62, 69 (3d Cir. 2000) (quoting *Mortensen*, 549 F.2d at 891).

Here, Paytime asserts a facial challenge to this Court's subject matter jurisdiction to hear the instant case.

III. FACTUAL SUMMARY

In accordance with the standard of review applicable to a Rule 12(b)(1) Motion to Dismiss, the following facts are derived from the complaints underlying the consolidated case and are viewed in the light most favorable to the Plaintiffs.

As the parties are aware, we issued an order consolidating these matters. In large part, the factual underpinnings are identical; however, where there are distinctions, we will identify those distinctions.

Paytime is a national payroll service company that offers a variety of services to its clients, including human resource management services, time and attendance systems, and web-based payroll submission. (*Storm*, Doc. 17, ¶ 6). Plaintiffs and putative class members are current or former employees of companies that used Paytime as their payroll processing service. (*Id.*, ¶¶ 8-11).

In order to facilitate payroll processing, Plaintiffs and the proposed class members were required to provide to their employers confidential personal and financial information, including their full legal names, addresses, bank account data, Social Security numbers, and dates of birth. (*Id.*, ¶ 14). This sensitive information was then provided to Paytime. (*Id.*, ¶ 15).

On April 7, 2014, unknown third parties gained unauthorized access to Paytime's computer systems. Paytime did not discover this security breach until

April 30, 2014. (*Id.*, ¶ 17). Plaintiffs further allege that Paytime waited until May 12, 2014 to begin to notify affected parties that there had been a security breach. (*Id.*, ¶ 18). On May 20, 2014, Paytime disclosed that forensic experts had conducted an investigation into the breach, and were able to confirm that the data breach had in fact occurred, and that the confidential personal information of employees of their clients had been accessed by these unknown third parties. (*Id.*, ¶ 19). Plaintiffs allege that nationally, over 233,000 individuals had their personal and financial information "misappropriated" as a result of the breach of Paytime's computer network. (*Id.*, ¶ 20).

Plaintiffs allege that as a result of this data breach, they and the proposed class members have spent, or will need to spend, time and money to protect themselves from identity theft. (*Id.*, ¶ 28). Plaintiffs assert they have suffered actual damages, as well. As an "example" of these damages, Plaintiffs point to Plaintiff Wilkinson, who is an employee of a government contractor and must have security clearances in order to perform his job. After Paytime's data breach, Wilkinson reported the incident to this employer, who then suspended his security clearances while the employer investigated the situation. (*Id.*, ¶ 29). During the investigation, Wilkinson was required to work at a different job site, resulting in a four hour increase in his daily commute. This increased commute caused Wilkinson to incur

travel expenses in addition to lost time. (*Id.*).

Plaintiffs in *Holt* allege similar injuries and actual damages, such as costs of monitoring their financial accounts, the opportunity cost of the time spent monitoring their accounts for identity theft, and costs of obtaining replacement checks and/or credit and debit cards. (*Holt*, Doc. 1, ¶ 40). They also allege as injuries "the significant possibility of monetary losses arising from unauthorized bank account withdrawals, fraudulent payments, and/or related bank fees charged to their accounts." (*Id.*, ¶ 36). As in *Storm*, they also allege as an injury the increased risk of identity theft. (*Id.*, ¶ 39).

Paytime has offered to provide free credit monitoring and identity restoration services for twelve (12) months for all persons affected by the data breach. (*Storm*, Doc. 37, Ex. B).

IV. DISCUSSION

First, we will consider whether Plaintiffs have standing to bring this case, based on the factual allegations of their Complaints. If none have standing, of course, we must dismiss the matter *sub judice*. If any Plaintiffs do have standing, we will then consider whether they have stated a claim for which relief can be granted.

Article III courts are courts of limited jurisdiction. As a constitutional

matter, federal courts only have jurisdiction over actual "cases or controversies." U.S. CONST. art. III, § 2. One element of this limitation is that plaintiffs have the burden of establishing they have standing to sue. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Standing analysis focuses on whether the "plaintiff is the proper party to bring this suit." *Raines v. Byrd*, 521 U.S. 811, 818 (1997) (citing *Simon v. Eastern Ky. Welfare Rights Organization*, 426 U.S. 26, 38 (1976)). More specifically, the classical formulation of standing requirements is that "a plaintiff must allege personal injury fairly traceable to the defendant's allegedly unlawful conduct and likely to be redressed by the requested relief." *Allen v. Wright*, 468 U.S. 737, 751 (1984). Procedurally, this translates to a requirement that a plaintiff must allege sufficient factual allegations in his or her complaint in order to establish standing. *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990).

The personal injury element of standing requires an "injury in fact"–one that is "concrete in both a qualitative and temporal sense," as opposed to merely "abstract." *Id.* The injury must also be actual or "imminent," not "conjectural" or "hypothetical." *Id.* (internal citations omitted). The imminency requirement has caused some consternation among the courts, leading the United States Supreme Court to expound on what an "imminent" injury entails in order to clarify this somewhat abstract concept. "Allegations of possible future injury do not satisfy the

requirements of Art. III. A threatened injury must be 'certainly impending' to constitute injury in fact." *Id.* at 158 (citing to a long history of Supreme Court cases standing for this proposition). Recently, in *Clapper v. Amnesty Intern. USA*, 133 S.Ct. 1138 (2013), the Supreme Court reiterated that a threatened injury must be "certainly impending." *Id.* at 1147.[4] This standard establishes a high bar for plaintiffs seeking to recover for injuries which have not in fact occurred, even if they appear likely or probable. With this rigorous standard, courts seek to "reduce the possibility of deciding a case in which no injury would have occurred at all." *Lujan*, 504 U.S. at 564 n.2.

The Third Circuit has provided guidance on standing and its imminency requirement for future injuries, specifically in the context of data breaches, as these have unfortunately become common occurrences in the modern world. The Third Circuit has held that in the event of a data breach, a plaintiff does not suffer a

[4] Plaintiffs correctly point out that the Supreme Court in *Clapper* included a footnote in their opinion which states that "in some instances," a "substantial risk" that the harm will occur would be sufficient to confer standing on a plaintiff. *Id.* at 1150 n.5. This teasing footnote does indeed invite confusion in standing jurisprudence. However, in the case before us, we choose to rely on the standard the Court relied on for its holding in *Clapper*, rather than a footnote. Furthermore, *Reilly*, discussed *infra*, provides us with precedential guidance on standing specifically in the context of data breach cases. And as point of fact, if we were to apply the "substantial risk" standard, Plaintiffs have not met that bar, either. They allege that an identity fraud research study found that "nearly 1 in 4 data breach letter recipients became a victim of identity fraud . . . ." (*Storm*, Doc. 17, ¶ 23). A 25 % chance of Plaintiffs becoming identity fraud victims is not a substantial risk. By Plaintiffs' own calculations, injury is not impending for 75% of victims of the Paytime breach. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, No. 12-347, 2014 WL 1858458, *7 (D. D.C. May 9, 2014).

harm, and thus does not have standing to sue, unless plaintiff alleges actual "misuse" of the information, or that such misuse is imminent. *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011). In *Reilly*, employees of a law firm brought a putative class action against a payroll processing firm, called Ceridian, after Ceridian suffered a security breach by an unknown hacker. *Id.* at 40. There, the plaintiffs harbored concerns about the breach because Ceridian had their personal and financial information stored as data, including the names of the plaintiffs, their Social Security numbers, and in some cases, their birth dates and bank account information. *Id.* Plaintiffs sued Ceridian under negligence and breach of contract theories of liability, alleging that due to the data breach, they were subject to an increased risk of identity theft, had incurred costs to monitor their credit activity, and suffered from emotional distress. *Id.*

The Third Circuit affirmed the district court's dismissal of the case, on the ground that the plaintiffs lacked Article III standing. *Id.* at 41. The circuit court reasoned that plaintiffs' alleged future harm resulting from the security breach was not sufficiently imminent to meet the threshold for standing–the risk of future injury was significantly attenuated, considering that it was "dependent on entirely speculative, future actions of an unknown third party." *Id.* at 42. The court pointedly elaborated:

> "We cannot now describe how Appellants will be injured in this case without beginning our explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will Appellants have suffered an injury." *Id.* at 43 (emphasis in original).

Thus, the Third Circuit requires its district courts to dismiss data breach cases for lack of standing unless plaintiffs allege actual misuse of the hacked data or specifically allege how such misuse is certainly impending. Allegations of increased risk of identity theft are insufficient to allege a harm. *Id.* at 43.

Turning again to the matter *sub judice*, we will review Plaintiffs' factual allegations from the Amended Complaint in the consolidated case, and any distinctive allegations from the Complaint in *Holt*, to decide whether they allege an injury that is either actual or imminent. Here, the factual allegations are remarkably similar to those of *Reilly*. Plaintiffs allege that their personal and financial data were "obtained" "by unknown third parties." (*Storm*, Doc. 17, ¶ 2). They allege that this information was "accessed without their authorization" and "misappropriated." (*Id.*, ¶¶ 16, 20). Plaintiffs allege that as a result of the data breach, they and the proposed class members "are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse." (*Id.*, ¶ 27). Additionally, they have spent, or foresee spending, time and money to protect themselves from identity theft. (*Id.*, ¶ 28). They also allege that some Plaintiffs and

proposed Class Members have suffered actual damages as a result of the data breach. They specifically cite one person, Plaintiff Wilkinson, who is employed by a government contractor. (*Id.*, ¶ 29). Wilkinson's job requires him to have security clearances. Plaintiffs allege that after reporting the data breach to his employer, Wilkinson's "security clearances had to be suspended for a period of time so that his employer could investigate the situation." Due to this situation, Wilkinson was required to work at a different job site than his usual one and his commute time was significantly increased, resulting in loss of time and travel expenses. (*Id.*).

Reviewing these allegations, the Court finds no factual allegation of misuse or that such misuse is certainly impending. Plaintiffs do not allege that they have actually suffered any form of identity theft as a result of the data breach–to wit, they have not alleged that their bank accounts have been accessed, that credit cards have been opened in their names, or that unknown third parties have used their Social Security numbers to impersonate them and gain access to their accounts. *See Reilly*, 664 F.3d at 45. In sum, their credit information and bank accounts look the same today as they did prior to Paytime's data breach in April 2014. Under *Reilly*, we find that Plaintiffs have not alleged an actual injury.

Plaintiffs argue that the different verbs used in their allegations, such as "stolen" and "misappropriated," distinguish their case from *Reilly* in such a way as

to create a cognizable harm, but this is a strained argument, which would require the Court to ignore the substance of the allegations. In the complaint at issue in *Reilly*, plaintiffs alleged that an "outside hacker" was able to "infiltrate" the defendant's security system and "gain access" to confidential and personal information of the plaintiffs. Complaint at ¶ 11, *Reilly v. Ceridian Corp.*, 2011 WL 735512 (D. N.J. Feb. 22, 2011) (No. 10-5142). In the matter *sub judice*, Plaintiffs somewhat artfully chose other verbs, but to draw a distinction of substance would require us to elevate the thesaurus above our logic and common sense. At the core of both cases, plaintiffs alleged a hacker broke into the defendant's data system and accessed it to some degree. Implicit in the *Reilly* complaint, of course, is that the access was without permission–thus, they also effectively alleged that the data was "misappropriated," as was alleged in the instant case. However, regardless of verbiage, Plaintiffs have only alleged the data was accessed by an unknown third party. There is no allegation that the hacker caused a new bank account or credit card to be opened in any of Plaintiffs' names, or any other form of identity theft. In other words, Plaintiffs have not alleged actual "misuse" of the data, which is the touchstone of the *Reilly* standard. *Reilly* draws a clear line in the sand in this context as to when a data breach becomes a harm. While some may argue that the line should be more favorable to plaintiffs and could perhaps be drawn at the

moment the data is accessed, that is not the extant standard.

Further, Plaintiffs' alleged harm–that they are now at an increased risk of identity theft–does not suffice to allege an imminent injury. *Reilly*, 664 F.3d at 43.[5] Perhaps this strict imminency standard has some wisdom, for even though Plaintiffs may indeed be at greater risk of identity theft, the data breach in this case occurred in April 2014–almost a year ago– and Plaintiffs have yet to allege that any of them have become actual victims of identity theft. Indeed, putting aside the legal standard for imminence, a layperson with a common sense notion of "imminence" would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future. [6]

Plaintiffs cite *Reilly*'s discussion of the facts of *Pisciotta v. Old National Bancorp.*, 499 F.3d 629 (7th Cir. 2007), and how they are distinguishable from those of *Reilly* itself, to argue that the harm in the instant case is more "imminent" by virtue of the fact the breach was done by skilled hackers working from

---

[5] "Appellants' allegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing." *Reilly*, 664 F.3d at 43 (citing to *Whitmore*, 495 U.S. at 158).

[6] The logic of this paragraph also applies to the allegation in *Holt* that one of Plaintiffs' injuries in fact or actual damages is "the significant possibility of monetary losses arising from unauthorized bank account withdrawals, fraudulent payments, and/or related bank fees charged to their accounts." (*Holt*, Doc. 1, ¶ 36). This is effectively just a more detailed form of alleging that Plaintiffs are at an increased risk of identity theft. Further, a "possibility" of monetary losses resulting from a data breach does not state a harm.

"foreign" IP addresses. First, even if the hackers here were more skilled or "malicious," although this seems to be quite a speculative assessment for a party or court to make, the fact remains that the harm of misuse has yet to occur, almost a year later, which undercuts the imminency argument. Further, we note that *Pisciotta* did not mention the imminency requirement for threatened injuries for constitutional standing purposes, so we do not find that court's reasoning particularly persuasive on this issue. *Reilly*, 664 F.3d at 44.

Based on the failure to allege facts showing a misuse of data or that such misuse is imminent, *Clapper* and *Reilly* direct us to dismiss Plaintiffs for lack of standing without too much hesitation. This disposition is in line with the vast majority of courts who have reviewed data breach cases where no misuse was alleged post-*Clapper*. *See, e.g.*, *In re SAIC*, 2014 WL 1858458, at *8 ("This is not to say that courts have uniformly denied standing in data-breach cases. Most cases that found standing in similar circumstances, however, were decided pre-*Clapper* or rely on pre-*Clapper* precedent and are, at best, thinly reasoned.") (citations omitted); *Strautins v. Trustwave Holdings, Inc.*, 27 F.Supp.3d 871 (N.D.Ill. 2014); *Polanco v. Omnicell, Inc.*, 988 F.Supp.2d 451 (D.N.J. 2013).

However, Plaintiffs point to one of themselves, Kyle Wilkinson, as someone who has suffered actual damages, or actual injury, due to the data breach,

ostensibly to create a foothold in our jurisdiction. His supposed damages, in the form of increased commute time and related expenses, although surely unfortunate, are merely a form of prophylactic costs the Supreme Court has warned cannot be used to "manufacture" standing, even if those costs are reasonable. *Clapper*, 133 S.Ct. at 1151. In *Clapper*, the Court reasoned, "Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending." *Id.* Wilkinson's preventive measure taken–working from a different job site while his security clearance was reviewed– is different in form but not in substance from the classic forms of preventive measures taken in data breach cases, such as credit monitoring. Based on the applicable precedent, there is still no misuse of his data, and thus no injury.

Although this stringent standard for standing does leave Wilkinson and the other Plaintiffs to foot the bill for their preventive measures taken[7], the logic of the doctrine is sound, and the application of it in the context of the recent rash of data breach cases makes its wisdom all the more clear. Hackers are constantly seeking to gain access to the data banks of companies around the world. Sometimes, they

[7] However, Paytime has arranged to provide free credit monitoring for 12 months for all persons affected by the data breach, so Plaintiffs will not in fact have to pay for many of their reasonable preventive costs. (Doc. 37, Ex. B).

are successful. Other times not. Despite many companies' best efforts and tremendous expense to secure and protect their data systems, an industrious hacker every so often may find a way to access their data. Millions of people, out of reasonable fear and prudence, may decide to incur credit monitoring costs and take other preventive steps, which the hacked companies often freely provide.[8] However, for a court to require companies to pay damages to thousands of customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to businesses. There is simply no compensable injury yet, and courts cannot be in the business of prognosticating whether a particular hacker was sophisticated or malicious enough to both be able to successfully read and manipulate the data and engage in identity theft. Once a hacker does misuse a person's personal information for personal gain, however, there is a clear injury and one that can be fully compensated with money damages. *See Reilly*, 664 F.3d at 45-46. In that situation, a plaintiff would be free to return to court and would have standing to recover his or her losses.

---

[8] Hayley Tsukayama, *Target says customers signing up for free credit monitoring after data breach*, WASH. POST, Jan. 13, 2014, http://www.washingtonpost.com/business/technology/target-says-customers-signing-up-for-free-credit-monitoring-after-data-breach/2014/01/13/99fcce60-7c83-11e3-95c6-0a7aa80874bc_story.html; Tara Siegel Bernard, *What Anthem Customers Should Do Next After the Data Breach*, N.Y.TIMES, Feb. 6, 2015, http://www.nytimes.com/2015/02/07/your-money/what-anthem-customers-should-do-next-after-data-breach.html.

Plaintiffs also contend that they have alleged actual injury based on harm to their privacy interest, in having their confidential personal information accessed by an unauthorized third party. "For a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party . . . if no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated." *In re SAIC Litig.*, 2014 WL 1858458, at * 19 (citing 5 C.F.R. § 297.102). Here, Plaintiffs do not allege that the unidentified hacker was actually able to view, read, or otherwise understand the data it accessed. They do not allege that their information was exposed in such a way as to make it easily viewed. *Reilly* addressed this issue as well, noting that it is speculative that the hacker "read, copied, or understood the data." 664 F.3d at 40. Consequently, Plaintiffs have not alleged that harm to their privacy interest is actual or imminent.

Because we conclude that Plaintiffs lack standing and thus must dismiss the case, we need not address Paytime's other arguments for dismissal made in their Motion.

V. CONCLUSION

In conclusion, Plaintiffs have failed to plead specific facts demonstrating they have standing to bring this suit under Article III. Consistent with our above

discussion, we will grant Paytime's motion to dismiss, as set forth more fully hereinabove and as follows. Because we are dismissing the instant case for lack of standing under Rule 12(b)(1), the dismissal is without prejudice.

A separate Order consistent with this Memorandum shall follow.